Secure Unidirectional File Transfer

A common need in a segmented network environment is to import and export files between different zones. File transfer and file sharing is done both between people and machines, using several different technologies depending on the environment. However, file transfer can quickly become a challenge when the zones also have different security classifications.

Challenge

Transferring files without exposing your sensitive environment

Any type of communication between security zones implies that one or more information flows must be allowed between the zones. Transferring files from a sensitive zone to a less sensitive, and less secure, zone risks exposing the sensitive zone to attacks originating from the less sensitive zone. The very existence of an information flow exposes systems on both sides of the flow to various security related risks.

Solution

Secure unidirectional file transfer

The solution is based on Advenica's SecuriCDS Data Diode DD1000i, a data diode ensuring unidirectional data transfer with built-in support for several file transfer protocols. Protocols can be combined in any way so that you can use e.g. SMB on one side and SFTP on the other side. The solution integrates with existing or newly installed servers or clients. In this regard, the DD1000i can be configured either as a server or client on the sender side (upstream) and as a client on the receiver side (downstream). For NFS and SMB there is only the choice to act as a client on the user side.

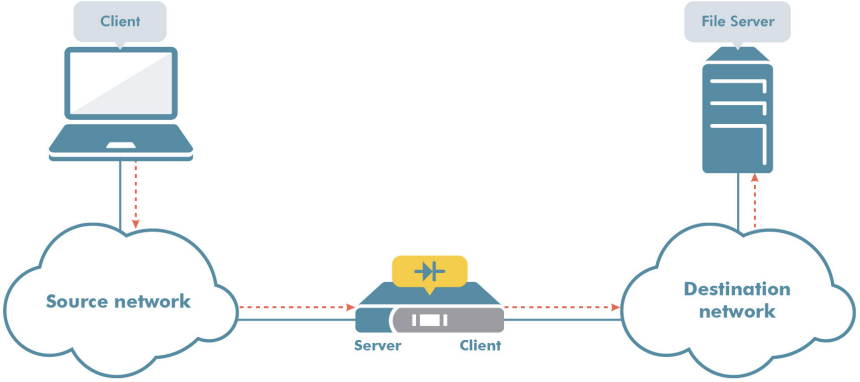

Figure 1: *DD1000i configured as server on sender side (upstream side) and client on receiver side/ downstream. Integration with client and server on each side.*

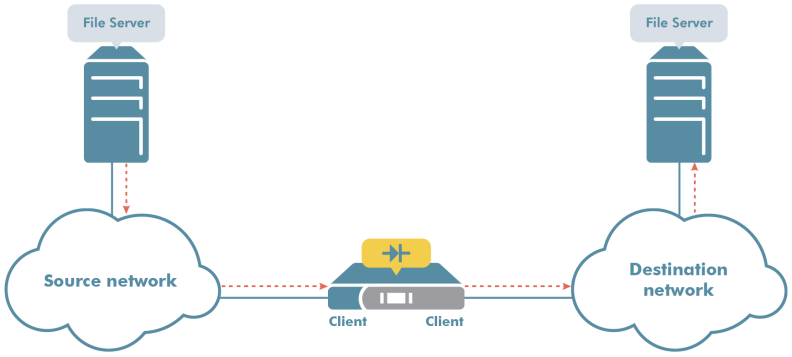

Figure 2: *DD1000i configured with clients on both sides. The DD1000i integrates with the file servers and continuously checks for new files on the sender's network. Files in a designated directory structure are transferred/mirrored from the source server to the destination server.*

The file name and a time stamp are logged with each file transfer.

Data Diode DD1000i with server

When the DD1000i acts as a server, clients can connect and upload files to the DD1000i. The DD1000i is configured with username and password, alternatively a certificate to be used for authentication of clients. If a directory structure is uploaded to the DD1000i, this entire structure will be copied/mirrored across the diode to the downstream side.

Data Diode DD1000i with client

When the DD1000i acts as a client upstream, it continuously checks (polls) for new files to transfer. The DD1000i is configured with the IP address of the file server and root directory of the directory structure to be copied. All directories and files below the root directory will be copied over the data diode. The DD1000i is configured with username and password, alternatively a certificate. You can choose whether you want to delete or keep copied files on the source server. You can also choose how often the client polls for new files. DD1000i acts as a client on the downstream side and files sent over the data diode will be uploaded to the configured server. DD1000i is configured with the address to the file server and root directory, as well as username/password, alternatively a certificate.

Advantages

File transfer solution with high assurance data diode technology

Advenica's SecuriCDS DD1000i provides a comprehensible and secure file transfer solution, enabling information flow from a sensitive zone to a less sensitive zone. The DD1000i supports several common file transfer protocols and integrates smoothly with existing file servers. The solution involves easy configuration of a full directory tree replication for which only changes to the file structure are transferred, minimising the amount of copied data and thereby required bandwidth.

Most importantly, the DD1000i guarantees with assurance at the highest level that information can only pass one-way from the source network to the destination network. This eliminates exposures and risks in the less secure destination network from spreading into the more sensitive source network. The one-way separation provided by the DD1000i is based on optical hardware and cannot be manipulated neither due to malware infections, nor misconfigurations.

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more on advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED